CLAIMS

What is claimed is:

1. A mating key gateway adapted to retrieve at least one mating key used to encrypt a program key that is used to scramble digital content prior to transmission to a digital device, comprising:

a bus;

a processor coupled to the bus;

an interface coupled to the bus, the interface being adapted to receive information from (1) a sender of the digital content and (2) either a server controlled by a supplier of the digital device or a trusted third party; and

a non-volatile storage unit coupled to the bus, the non-volatile storage unit to store a mating key lookup table to identify either the server controlled by the supplier of the digital device or the trusted third party based on the information received from the sender.

2. The mating key gateway of claim 1, wherein the interface to receive the information from the sender being one of a cable provider, a satellite-based provider, a terrestrial-based provider, an Internet service provider and a conditional access (CA) provider operating with one of the cable provider, the satellite-based provider, the terrestrial-based provider and the Internet service provider.

3. The mating key gateway of claim 2, wherein the interface to receive information from the supplier being a manufacturer of the digital device.

4. The mating key gateway of claim 2, wherein the information received by the interface from the sender

comprises a mating key generator being a message that comprises an identifier of the supplier.

5. The mating key gateway of claim 4, wherein the mating key generator received by the interface further comprises an identifier of a provider of a system that enables transmission of both the digital content and the mating key generator to the digital device.

6. The mating key gateway of claim 5, wherein the mating key generator received by the interface further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the digital content and the mating key generator are transmitted, and (ii) a mating key sequence number.

7. The mating key gateway of claim 1, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of serial numbers for digital devices supplied by each supplier of a plurality of suppliers including the supplier, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including information to establish communications with a server controlled by one of the plurality of suppliers.

8. The mating key gateway of claim 1, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of serial numbers for digital devices supplied by each supplier of a plurality of suppliers including the supplier, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including an address to establish

communications with a trusted third party authorized by one of the plurality of suppliers.

9. The mating key gateway of claim 4, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of mating key generators for digital devices supplied by each supplier of a plurality of suppliers including the supplier, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including information to establish communications with a server controlled by one of the plurality of suppliers.

10. The mating key gateway of claim 9, wherein the information includes an address to establish communications over a network.

11. The mating key gateway of claim 4, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of mating key generators for digital devices supplied by each supplier of a plurality of suppliers including the supplier, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including at least one mating key uniquely corresponding to one of the mating key generators.

12. A mating key gateway adapted to retrieve a mating key used to encrypt a program key that is used to scramble digital content prior to transmission to a digital device, the mating key gateway comprising:

a processor;

an interface in communication with the processor, the interface being adapted to exchange information with (1) a

headend and (2) a server configured to store a mating key associated with the digital device; and

a non-volatile storage unit to store a mating key lookup table to identify the server based on the information received from the headend.

13. The mating key gateway of claim 12, wherein the interface receives the mating key from the server being controlled by a manufacturer of the digital device.

14. The mating key gateway of claim 13, wherein the information received by the interface from the headend comprises a mating key generator being a message that comprises an identifier of the manufacturer of the digital device.

15. The mating key gateway of claim 14, wherein the mating key generator received by the interface further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the digital content and the mating key generator are transmitted, and (ii) a mating key sequence number.

16. The mating key gateway of claim 12, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of serial numbers of digital devices supplied by each of a plurality of manufacturers, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including information to establish communications with a server controlled by one of the plurality of manufacturers.

17. The mating key gateway of claim 16, wherein the server controlled by one of the plurality of manufacturers is the server.

18. The mating key gateway of claim 14, wherein the mating key lookup table stored by the non-volatile storage unit comprises (i) a first group of entries forming a range of mating key generators associated with digital devices supplied by each of a plurality of manufacturers, and (ii) a second group of entries corresponding to the first group of entries, each entry of the second group of entries including information to establish communications with a server controlled by one of the plurality of manufacturers.

19. The mating key gateway of claim 18, wherein the information includes an address to establish communications over a network.

20. The mating key gateway of claim 12 being adapted to additionally store mating keys for selected digital devices.

21. A secure content delivery system comprising:

a trusted third party to store a plurality of mating keys associated with digital devices, each mating key being used to encrypt a key that is used to scramble digital content; and

a mating key gateway in communications with the trusted third party, the mating key gateway to provide information received from a headend to the trusted third party for retrieval of a requested mating key.

22. The secure content delivery system of claim 21, wherein the key used to scramble the digital content is a program key.

23. The secure content delivery system of claim 22, wherein the information provided to the trusted third party comprises a mating key generator being a message

that comprises an identifier of a supplier of one of the digital devices.

24. The secure content delivery system of claim 23, wherein the identifier of the supplier included in the mating key generator identifies a manufacturer of the one of the digital devices.

25. The secure content delivery system of claim 23, wherein the mating key generator provided to the trusted third party further comprises an identifier of a provider of the secure content delivery system that enables transmission of both the digital content and the mating key generator to the one of the digital devices.

26. The secure content delivery system of claim 23, wherein the mating key generator provided to the trusted third party further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the digital content and the mating key generator are transmitted, and (ii) a mating key sequence number.

27. A method comprising:

receiving a mating key generator; and

outputting a mating key based on the mating key generator and an one-time programmable value being identical to a key stored in a digital device of a set-top box targeted to receive information encrypted with either the mating key or a derivative of the mating key.

28. The method of claim 27, wherein prior to outputting the mating key, the method further comprises:

receiving a serial number being used to locate the one-time programmable value.

29. The method of claim 27, wherein prior to outputting the mating key, the method further comprises:

computing the mating key by performing a computation on the mating key generator and the one-time programmable value to produce the mating key.

30. The method of claim 27, wherein the mating key generator includes at least one of (i) a first identifier to identify a manufacturer of the digital device, (ii) a service provider identifier, (iii) a conditional access provider identifier, and (iv) a mating key sequence number.

31. The method of claim 27, wherein prior to outputting the mating key, the method further comprises:

computing the mating key by performing a computation on the mating key generator and the one-time programmable value.

32. A conditional access (CA) control system in communication with a mating key server, the CA control system comprising:

means for receiving a mating key from the mating key server, the mating key being computed based on a mating key generator and a one-time programmable value; and

means for producing a plurality of derivatives keys based on the mating key, each derivative key being used to encrypt a key that is configured to descramble digital content targeted for a digital device of a set-top box.

33. The CA control system of claim 32, wherein the key configured to descramble the digital content is a program key.

34. The CA control system of claim 32 further comprising:

transmitting the encrypted program key and the scrambled digital content to the digital device of the set-top box.

35. A method comprising:

receiving a request for a key over a communication bus;

recovering different versions of the key depending on which of a plurality of providers is requesting the key; and

providing the different versions of the key to the plurality of providers adapted to use the key as either a mating key to encrypt digital content delivered to a targeted digital device or as a precursor key to derive the mating key to encrypt the digital content delivered to the targeted digital device.

36. The method of claim 35, wherein the recovering of the key includes accessing a database to retrieve the key being a pre-calculated value.

37. The method of claim 35, wherein the recovering of the key includes calculating the key substantially in real time based on a unique key associated with the targeted digital device, an identical copy of the unique key being permanently stored within the targeted digital device.

38. The method of claim 35, wherein the providing of the key is transmitted to at least one conditional access provider, to at least one service provider or to at least one conditional access provider and at least one service provider.